



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,125	01/31/2002	James Kleinstein	112-0039US	2526

29855 7590 10/18/2006

WONG, CABELLO, LUTSCH, RUTHERFORD & BRUCCULERI,
L.L.P.
20333 SH 249
SUITE 600
HOUSTON, TX 77070

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 10/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/062,125

Applicant(s)

KLEINSTEIBER ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 August 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-61 and 72-87 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 January 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 2/21/2006, 4/27/2006.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

1 This action is in response to the communication filed on 8/2/2006.

2 **DETAILED ACTION**

3 ***Response to Arguments***

4 Applicant's arguments filed 5/12/2006 and 8/2/2006 have been fully considered but they
5 are not persuasive.

6 Regarding applicants' argument that based on the specification, one of ordinary skill in
7 the art would be able to determine the scope of "secure location", "less secure location", and
8 "substantive communication", the examiner does not find the argument persuasive. As
9 previously pointed out, the specification, including the sections pointed to by the applicants in
10 the communication dated 5/12/2006, do not define the terms in such a way that one of ordinary
11 skill in the art would be able to determine the scope of what is being claimed. This is because
12 the terms are relative, and no specific boundaries have been established by the specification in
13 order to make certain what does and does not fall within the scope of the limitations. As a
14 further example, **is a locked room in Antarctica a more secure location than a plaza guarded**
15 **by armed police officers?** One person may consider this question and say "yes" while another
16 may say "no", because the term "secure" depends on a personal interpretation of what is secure,
17 and therefore the term "secure" is relative. As such, the examiner does not find the arguments
18 persuasive.

19 Regarding applicants' argument that Sudama does not teach "locating one or more nodes
20 in a secure location", or "locating one or more nodes in a less secure location" the examiner does
21 not find the arguments persuasive. Sudama disclosed that "management operations can follow a
22 trusted path downstream...however, no trusted path exists for routing management operations

Art Unit: 2131

1 upstream.” [Sudama Col. 8 Paragraph 4] As such, the upstream nodes are in a more secure
2 location than the downstream locations. Therefore, the examiner does not find the arguments
3 persuasive.

4 Regarding applicants’ argument that Sudama did not disclose “a first port on a first node
5 sending said management information to a second port on a second node via a communication
6 media exclusively shared by said first port and said second port” the examiner does not find the
7 argument persuasive. In Fig. 2, the first node is M1 and the second node is M2. The
8 communication media is Link 44, and the ports are the inherent ports which allow for the
9 interface between Link 44 and M1 and M2. As there is no indication that there is any link
10 between M1 and M2 other than link 44, it is exclusively shared, and therefore Sudama meets the
11 limitations of the claim language. See Sudama Col. 10 Paragraph 4 for further support.

12 Regarding applicants’ argument that Sudama did not disclose “determining a first list of
13 nodes that may send or receive substantive communication in the secure network”, the examiner
14 does not find the argument persuasive. The trusted routing paths of Sudama meet the limitation
15 of the claim language as they determine which nodes may receive management operations.
16 Therefore, the examiner does not find the argument persuasive.

17 Regarding applicants’ argument that Sudama did not disclose a primary configuration
18 node configured or adapted to exclusively control a defined set of management functions
19 throughout said secure network, the examiner does not find the argument persuasive. Sudama,
20 as seen in Col. 8 Paragraph 4) disclosed that M1 exclusively controls the management functions
21 of S1 (C1), and as such meets the limitations of the claim language.

1 Regarding applicants' arguments against the rejection of claim 72, the arguments are
2 moot in view of new grounds of rejection necessitated by applicants' amendments.

3 Regarding applicants' argument that Sudama did not disclose that the management
4 devices perform switching functions, the examiner does not find the argument persuasive. The
5 claim language does not require a switch, but rather requires at least one of switching and routing
6 devices. Sudama disclosed that the management devices performed routing operations and
7 therefore meets the limitations of the claim. Furthermore, although "switching and routing
8 devices" are claimed, there is no functionality claimed of such devices and as such, any device
9 operating in a manner as claimed of the devices, whether called a "switch" or not would meet the
10 limitations of the claim.

11 Regarding applicants' argument that Sudama did not disclose devices able to inter-
12 communicate by direct link and by forwarding through, the examiner does not find the argument
13 persuasive. Sudama clearly disclosed this in Col. 8 Paragraph 4 where Sudama disclosed routing
14 communications from M1 to M4 via trusted paths, and as can be seen in Fig. 2, the paths include
15 passing through other devices.

16 Regarding applicants' argument that Sudama did not disclose "all of said devices
17 carrying a list of all devices allowed on the network", the examiner does not find the argument
18 persuasive. Sudama disclosed that each management server stored a list of trusted relations
19 between the management servers. These lists include the devices of the network and therefore
20 meet the limitations of the claim. As such, the examiner does not find the argument persuasive.

21 Regarding applicants' argument that Sudama did not disclose a "logical management
22 channel" which may be disabled through network management control, the examiner does not

Art Unit: 2131

1 find the argument persuasive. The fact that the management control of Sudama prevents
2 upstream management communication, shows that the management communications are separate
3 from non management communications and therefore in a “logical channel” and the upstream
4 “channel” is disabled through the list of trusted paths. As such the examiner does not find the
5 argument persuasive.

6 Regarding applicants’ argument that Sudama did not disclose an NCE list and a SCC list,
7 the examiner does not find the argument persuasive. There is no requirement in the claim that
8 these lists cannot be one in the same. As the list of Sudama includes all of what is required by
9 the NCE and SCC lists, Sudama meets the limitation of the claim. Sudama disclosed indication
10 of each device in the network that may operate as said network configuration entity in Col. 5
11 Paragraph 3 wherein it was disclosed that “a list of hosts for performing specified functions, **the**
12 **hosts designated management servers...**”. Furthermore Sudama disclosed an indication of
13 each device allowed to participate in said secure network, which can be seen in Col. 5 Paragraph
14 3, wherein Sudama disclosed “a list of hosts for performing specified functions”. These are the
15 hosts in the “secure” network. Therefore, the examiner does not find the arguments persuasive.

16 All rejections and objections not set forth below have been withdrawn.

17 Claims 1-61 and 72-87 have been examined and claims 62-71 and 88-89 have been
18 cancelled.

19 ***Claim Rejections - 35 USC § 112***

20 The following is a quotation of the second paragraph of 35 U.S.C. 112:

21 *The specification shall conclude with one or more claims particularly pointing out and*
22 *distinctly claiming the subject matter which the applicant regards as his invention.*
23

1 Claims 1-61, 72, and 76-78 are rejected under 35 U.S.C. 112, second paragraph, as being
2 indefinite for failing to particularly point out and distinctly claim the subject matter which
3 applicant regards as the invention.

4 The term "secure location" in claims 1, 13, is a relative term which renders the claim
5 indefinite. The term "secure location" is not defined by the claim, the specification does not
6 provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would
7 not be reasonably apprised of the scope of the invention. In this particular instance, one of
8 ordinary skill in the art would be unable to determine what constitutes "a secure location". For
9 example, would a fireproof room be considered a secure location. Would a room anchored to the
10 earth be considered a secure location. Would a plaza with armed guards be considered a secure
11 location. As such, one of ordinary skill in the art would not be able to determine the scope of the
12 claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the
13 subject matter which the applicant regards as the invention.

14 The term "less secure location" in claims 1, 13 is a relative term which renders the claim
15 indefinite. The term "less secure location" is not defined by the claim, the specification does not
16 provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would
17 not be reasonably apprised of the scope of the invention. In this particular instance, one of
18 ordinary skill in the art would be unable to determine what constitutes "a less secure location".
19 For example, would a non-fireproof room be considered a less secure location. Would a room
20 not anchored to the earth be considered a less secure location. Would a plaza with no armed
21 guards be considered a less secure location. Furthermore, the claim gives no basis as to what the
22 location is less secure than. As such, one of ordinary skill in the art would not be able to

determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

The term "substantive" in claims 1, 18, 19, 35, 72, and 76 is a relative term which renders the claim indefinite. The term "substantive" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what is considered substantive communication. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claims 1, 18, 19, 35, 72, and 76 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claims 2-34, 36-61, and 77-78 are rejected by virtue of their dependency to an above rejected claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-13, 17-19, 35- 47, 51-53, and 73 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudama et al. (US Patent Number 5,619,657) hereinafter referred to as Sudama.

Art Unit: 2131

1 Regarding claim 1, Sudama disclosed a method of operating a secure network having
2 plurality of network nodes, each node comprising one or more ports (See Sudama Abstract), the
3 method comprising the steps of: locating one or more nodes in a secure location (See Sudama
4 Fig. 2); locating one or more nodes in a less secure location (See Sudama Col. 8 Paragraph 4);
5 communicating selected management information from a primary configuration node to all other
6 nodes in the secure network (See Sudama Col. 5 Paragraph 3), said communicating having the
7 sub-steps of, a first port on a first node sending said management information to a second port on
8 a second node via an communication media exclusively shared by said first port and said second
9 port (See Sudama Col. 8 Paragraph 4 and Fig. 2); allowing no management access to said secure
10 network from nodes located in said less secure locations (See Sudama Col. 8 Paragraph 4 and
11 Fig. 2); determining a first list of nodes that may send or receive substantive communication in
12 the secure network (See Sudama Col. 5 Paragraph 3); and prior to substantive communication
13 between any two directly-connected ports, authenticating a link between said directly connected
14 ports (See Sudama Col. 5 Paragraph 3).

15 Regarding claim 35, Sudama disclosed a specific networking node operating in a secure
16 network, said secure network having a plurality of network nodes, each node comprising one or
17 more ports (See Sudama Fig. 2 and Abstract), said specific networking node comprising: a first
18 port on said specific networking node for receiving selected management information from a
19 primary configuration node (See Sudama Col. 5 Paragraph 3 and Fig. 2), said first port directly
20 communicating with a second port on a second node via an communication media exclusively
21 shared by said first port and said second port (See Sudama Fig. 2 and Col. 8 Paragraph 4); a
22 memory for storing (i) management access information (See Sudama Col. 8 Paragraph 1), and

Art Unit: 2131

1 (ii) device connection information specifying nodes or ports that may send or receive substantive
2 communication in the secure network (See Sudama Col. 8 Paragraph 1); and a processor for
3 causing the authentication of the link between said first port and said second port prior to
4 substantive communication between said first and second ports (See Sudama Col. 5 Paragraph
5 3).

6 Regarding claim 73, Sudama disclosed a network comprising: a plurality of devices
7 including one or more switching and routing devices (See Sudama Col. 5 Paragraph 3), any two
8 of said devices able to inter-communicate only by direct links between each other (See Sudama
9 Fig. 2), all devices able to inter-communicate by forwarding communications through each other
10 (See Sudama Col. 5 Paragraph 3); all of said devices capable of mutually authenticating directly
11 connected links (See Sudama Col. 5 Paragraph 3); one or more pre-designated devices for
12 facilitating management-level control of the network (See Sudama Col. 5 Paragraph 3); and all
13 of said devices carrying a list of all devices allowed on the network (See Sudama Col. 8
14 Paragraph 1), wherein said primary configuration node is configured or adapted to exclusively
15 control a defined set of management functions throughout said secure network (See Sudama Col.
16 5 Paragraph 3).

17 Regarding claims 2-12, and 36-46, Sudama disclosed that said set of management
18 functions comprising the recognition, operation and succession of primary configuration node
19 (See Sudama Col. 5 Lines 20-21); node connection controls for designating nodes to participate
20 in the secure network (See Sudama Col. 4 Lines 28-31), device connection controls that indicate
21 port relationships in said secure network (See Sudama Col. 5 Lines 22-23), and management

1 access controls that restrict management services to a defined set of endpoints (See Sudama Col.
2 5 Lines 20-23).

3 Regarding claims 13, and 47, Sudama disclosed that the step of allowing no management
4 access to said secure network from nodes located in said less secure locations comprises the sub-
5 step of distributing a MAC list to every node in said secure network, said MAC list comprising
6 an indication of network endpoints from which management access is acceptable (See Sudama
7 Col. 5 Paragraph 3 and Fig. 2).

8 Regarding claims 17 and 51, Sudama disclosed that the network endpoints comprise
9 uniquely identified nodes resident in said secure network (See Sudama Fig. 2 and Col. 5
10 Paragraph 3).

11 Regarding claims 18 and 52, Sudama disclosed that the step of determining a first list of
12 nodes that may send or receive substantive communication in the secure network comprises the
13 sub-step of distributing a DCC list to every node in said secure network, said DCC list
14 comprising definitions that logically bind a port on said primary configuration node to one or
15 more other ports resident in the secure network (See Sudama Col. 5 Paragraph 3 and Col. 8
16 Paragraph 1 and Fig. 2).

17 Regarding claims 19 and 53, Sudama disclosed that the step of determining a first list of
18 nodes that may send or receive substantive communication in the secure network comprises the
19 sub-step of distributing a DCC list to every node in said secure network, said DCC list
20 comprising definitions that logically bind each port in said secure network to one or more other
21 ports resident in said network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig.
22 2).

1 ***Claim Rejections - 35 USC § 103***

2 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
3 obviousness rejections set forth in this Office action:

4 *A patent may not be obtained though the invention is not identically disclosed or*
5 *described as set forth in section 102 of this title, if the differences between the subject matter*
6 *sought to be patented and the prior art are such that the subject matter as a whole would have*
7 *been obvious at the time the invention was made to a person having ordinary skill in the art to*
8 *which said subject matter pertains. Patentability shall not be negated by the manner in which*
9 *the invention was made.*
10

11 Claims 14-16, 20-21, and 48-50, and 54-55 are rejected under 35 U.S.C. 103(a) as being
12 unpatentable over Sudama. Sudama disclosed distributing a list of management acceptable nodes
13 in a network (See Sudama Col. 5 Paragraph 3), but failed to disclose that the nodes comprise IP
14 addresses, that IP addresses are associated with SNMP or Telnet or HTTP or API, or that the
15 nodes had ports which were uniquely identified by a world wide name. However, it was well
16 known in the art at the time of invention that network nodes have IP addresses, that IP addresses
17 are associated with access from SNMP or Telnet or HTTP or API, and that network ports were
18 uniquely identified by a world wide name. . Therefore, it would have been obvious to the
19 ordinary skill in the art at the time of invention to employ these well known networking features
20 in the network of Sudama.

21 Claims 22-31, 33-34, 56-61, and 76-87 are rejected under 35 U.S.C. 103(a) as being
22 unpatentable over Sudama as applied to claim 1 above, and further in view of FIPS PUB 196
23 (“Entity Authentication Using Public Key Cryptography”) hereinafter referred to as FIPS.

1 Regarding claims 22 and 56, Sudama disclosed mutual authentication performed between
2 the network devices (See Sudama Col. 5 Paragraph 3) but failed to disclose the use of a three
3 pass authentication scheme in order to do so.

4 FIPS teaches a method for mutual authentication comprising sending a first fact (R_B)
5 from said first port to said second port (See FIPS Section 3.3 Step 2); at said second node,
6 creating a second-type derivative of said first fact (sS_A), sending said second-type derivative of
7 said first fact from said second port to said first port (See FIPS Section 3.3 Step 3); at said first
8 node, storing said second-type derivative of said first fact in a first memory; sending a second
9 fact (R_A) from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node,
10 creating a first-type derivative of said second fact (sS_B); sending said first-type derivative of said
11 second fact from said first port to said second port (See FIPS Section 3.3 Step 5); at said second
12 node, storing said first-type derivative of said second fact in a second memory; sending defined
13 information concerning said first node (CertB) from said first port to said second port (See FIPS
14 Section 3.3 Step 5); sending a third-type derivative of said defined information concerning said
15 first node from said first port to said second port (It was well known that certificates included
16 signatures of the hash of the certificate); at said second node, comparing said defined
17 information concerning said first node with said third-type derivative of said defined information
18 concerning said first node (It was also well known to verify the signature of the certificate at the
19 receiver); at said second node, comparing said first type derivative of said second fact with said
20 second fact (See FIPS Section 3.3 Step 6); sending defined information concerning said second
21 node (CertA) from said second port to said first port; sending a third-type derivative of said
22 defined information concerning said second node from said second port to said first port (It was

1 well that certificates included signatures of the hash of the certificate); at said first node,
2 comparing said defined information concerning said second node with said third-type derivative
3 of said defined information concerning said second node (It was also well known to verify the
4 signature of the certificate at the receiver); and at said first node, comparing said second type
5 derivative of said first fact with said first fact (See FIPS Section 3.3 Step 4).

6 It would have been obvious to the ordinary person skilled in the art at the time of
7 invention to employ the teachings of FIPS as the mutual authentication of Sudama. This would
8 have been obvious because the ordinary person skilled in the art would have been motivated to,
9 mutually authenticate the nodes prior to communication between the nodes.

10 Regarding claim 76, the combination of Sudama and FIPS disclosed a routing device for
11 receiving and directing information in a network (See Sudama Fig. 2), comprising: a public and
12 private key pair (See FIPS Section 3.1.4); one or more ports for coupling to other routing devices
13 and for authenticating said other routing devices and for communicating using said public and
14 private key pair (See Sudama Fig. 2 and Col. 5 Paragraph 3 and the rejection of claim 22 above);
15 a memory for storing a list of all said other routing devices that are allowed to substantively
16 communicate on the network (See Sudama Col. 8 Paragraph 1); and a least one logical
17 management access channel that may be disabled through network management control (See
18 Sudama Col. 8 Paragraph 4).

19 Regarding claim 79, the combination of Sudama and FIPS disclosed a network
20 configuration entity configured or adapted to exclusively control a defined set of management
21 functions throughout a secure network, said secure network comprising a plurality of switching
22 devices, said set of management functions comprising (i) the recognition, operation and

Art Unit: 2131

1 succession of the network configuration entity and (ii) switch connection controls for designating
2 devices to participate in the secure network (See Sudama Col. 5 Paragraph 3), said network
3 configuration entity comprising; a memory for storing an NCE list, said NCE list comprising an
4 indication of each device in the network that may operate as said network configuration entity
5 (See Sudama Col. 5 Paragraph 3); an SCC list, said SCC list comprising an indication of each
6 device allowed to participate in said secure network (See Sudama Col. 5 Paragraph 3); a first
7 secret fact; a first port for sending said secret fact to a second switch; a second port for receiving,
8 a second-type derivative of said first secret fact from said second switch, pre-defined information
9 about said second switch, and a third-type derivative of said pre-defined information about said
10 second switch; and a processor for (i) causing a comparison between said first secret fact and
11 said second-type derivative of said first secret fact, and (ii) causing a comparison between said
12 pre-defined information about said second switch and said third-type derivative of said pre-
13 defined information about said second switch (See the rejection of claim 22 above).

14 Regarding claims 23, 33, 58, and 81, the combination of Sudama and FIPS disclosed that
15 the step of comparing said defined information concerning said second node with said third-type
16 derivative of said defined information concerning said second node, comprises the sub-steps of:
17 reversing the derivation of the third-type derivative of said defined information concerning said
18 second node; and comparing the result of said reversal with said defined information concerning
19 said second node (It was well known at the time of invention that a signature was decrypted
20 using the public key of the certificate authority and compared with the signed data to verify the
21 signature).

1 Regarding claims 24, 59, and 82, the combination of Sudama and FIPS disclosed that the
2 step of comparing said defined information concerning said second node with said third-type
3 derivative of said defined information concerning said second node, comprises the sub-steps of:
4 making a third-type derivative of said defined information concerning said second node; and
5 comparing the made third-type derivative with the received third-type derivative (It was well
6 known at the time of invention that a signed hash was decrypted using the public key of the
7 certificate authority and compared with the hash of the certificate to verify the signature).

8 Regarding claim 25-27, the combination of Sudama and FIPS disclosed that the step, at
9 said second node, of creating a second-type derivative of said first fact comprises the sub-steps
10 of: encoding said first fact to yield an encoded first fact; and encrypting said encoded first fact (It
11 was well known at the time of invention that a signature was created by hashing the data to be
12 signed and then encrypting the hash with a private key of a public key pair).

13 Regarding claims 28-29, and 85, the combination of Sudama and FIPS disclosed that
14 defined information concerning said first node comprises encryption key information and that
15 encryption key information comprises a public key uniquely associated with said first node (See
16 FIPS Section 3.1.4).

17 Regarding claims 30-31, 34, 61, and 84, the combination of Sudama and FIPS disclosed
18 that the third-type derivative is created using a private key uniquely associated with an
19 encryption key authority, said encryption key authority associated with said first node and said
20 second node (See FIPS Section 3.1.4).

21 Regarding claims 57, and 80, Sudama and FIPS disclosed that the third port and the
22 fourth port are the same port (See Sudama Fig. 2).

1 Regarding claim 60, Sudama and FIPS disclosed that the second-type derivative is
2 associated with the third node (See FIPS Section 3.3 Step 3).

3 Regarding claim 77, Sudama and FIPS disclosed that the certificate authority for the
4 public and private key pair is not the entity controlling management access to said routing device
5 (See FIPS Section 3.1.4).

6 Regarding claim 78, Sudama and FIPS disclosed a memory for storing distributed time
7 service information (It was well known in the art for network devices to contain network time
8 service information).

9 Regarding claim 83, Sudama and FIPS disclosed that the second-type derivative is
10 associated with said second switch (See FIPS Section 3.3).

11 Regarding claims 86-87, Sudama and FIPS disclosed that the first secret fact is a random
12 nonce (See FIPS Section 3.3).

13 Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama and FIPS
14 as applied to claim 30 above, and further in view of Fischer (US Patent Number 5,422,953).

15 Sudama and FIPS disclosed the use of certificates (See the rejection of claim 22 above),
16 but failed to disclose the certificate being issued by the manufacturer of the node devices.

17 Fischer teaches that a manufacturer of a device can also be the issuer of the devices
18 public key certificate (See Fischer Col. 6 Paragraph 3).

19 It would have been obvious to the ordinary person skilled in the art at the time of
20 invention to employ the teachings of Fischer in the network system of Sudama and FIPS by
21 having the manufacturer of the network devices issue the certificates to the devices. This would

Art Unit: 2131

1 have been obvious because the ordinary person skilled in the art would have been motivated to
2 provide assurance through the certificate that network device was secure.

3 Claims 72 and 74 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama
4 as applied to claim 73 above, and further in view of Thapar et al. (US Patent Number 5,694,615)
5 hereinafter referred to as Thapar.

6 Sudama disclosed a method of securing a fabric, said fabric having a plurality of switches
7 all communicatively coupled together, said method comprising the steps of: only allowing
8 communication between pre-defined pairs of said devices as specified by a network operator
9 (See Sudama Col. 5 Paragraph 3); and only allowing substantive communication between
10 devices that are on a pre-defined list of allowed devices (See Sudama Col. 5 Paragraph 3), said
11 pre-defined list stored on a memory in each of said plurality of devices (See Sudama Col. 8
12 Paragraph 1); and only allowing substantive communication between directly connected ports
13 that have been mutually authenticated (See Sudama Col. 5 Paragraph 3), but failed to disclose
14 the system being used in a fibre channel.

15 Thapar teaches that the fibre channel addresses the need for very fast data transfers (See
16 Thapar Col. 1 Lines 18-26).

17 It would have been obvious to the ordinary person skilled in the art at the time of
18 invention to employ the teachings of Thapar in the communication network of Sudama by
19 replacing the routers of Thapar with Fibre Channel routers. This would have been obvious
20 because the ordinary person skilled in the art would have been motivated to allow for very fast
21 transfers of large volumes of data.

1 Claim 75 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as
2 applied to claim 73 above, and further in view of applicant admitted prior art.

3 Sudama disclosed a network of routers (See Sudama Fig. 2), but failed to disclose the
4 routers being in locked rooms.

5 Applicants admitted on page 2 paragraph 2 of the specification that the prior art secured
6 computer equipment by locking it in a room.

7 It would have been obvious to the ordinary person skilled in the art at the time of
8 invention to employ the teachings of the applicants' admitted prior art in the networking system
9 of Sudama by locking the management devices in rooms. This would have been obvious
10 because the ordinary person skilled in the art would have been motivated to protect the devices
11 against tampering and theft.

12 *Conclusion*

13 Claims 1-61 and 72-87 have been rejected.

14 Applicant's amendment necessitated the new ground(s) of rejection presented in this
15 Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).
16 Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

17 A shortened statutory period for reply to this final action is set to expire **THREE**
18 **MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**
19 **MONTHS** of the mailing date of this final action and the advisory action is not mailed until after
20 the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period
21 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
22 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

1 however, will the statutory period for reply expire later than SIX MONTHS from the date of this
2 final action.

3 Any inquiry concerning this communication or earlier communications from the
4 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.

5 The examiner can normally be reached on M-F 8-4.

6 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
7 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
8 organization where this application or proceeding is assigned is 571-273-8300.

9 Information regarding the status of an application may be obtained from the Patent
10 Application Information Retrieval (PAIR) system. Status information for published applications
11 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
12 applications is available through Private PAIR only. For more information about the PAIR
13 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
14 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would
15 like assistance from a USPTO Customer Service Representative or access to the automated
16 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

17
18
19
20
21 Matthew Henning
22 Assistant Examiner
23 Art Unit 2131
24 10/4/2006


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100